

CLAIMS

What is claimed is:

1. A data processing method for generating a digital signature, the method comprising the computer-implemented steps of:
 - receiving and transiently storing a first integer data value relating to a digital signature of an electronic message;
 - digitally computing a multiplicative inverse of the first integer data value modulo a prime modulus data value by computing a first quantity modulo the prime modulus data value;wherein the first quantity substantially equals, modulo the prime modulus data value, the first integer data value raised to a power of a second quantity;
wherein the second quantity is two less than the prime modulus data value; and
storing the multiplicative inverse in a computer hardware storage element for use in determining the digital signature of the electronic message.
2. A method for generating a digital output signal indicating a multiplicative inverse of an integer data value modulo a prime modulus, the method comprising the steps of:
 - receiving a first signal, indicating a value of the integer data value, at a base input of a modulo exponentiation block of an electronic integrated circuit;
 - sending a second signal, indicating a value of the prime modulus, to a modulus input of the modulo exponentiation block; and
 - sending a third signal, indicating a value of the prime modulus less two, to an exponent input of the modulo exponentiation block;wherein the modulo exponentiation block generates an output based on a first quantity modulo a value at the modulus input; and
wherein the first quantity substantially equals, modulo the value at the modulus input, a value at the base input raised to a power of a value at the exponent input.

1 3. A method for fabricating an electronic circuit that generates an output signal
2 indicating a multiplicative inverse of an integer data value modulo a prime modulus, the
3 method comprising the steps of:
4 connecting a first register holding signals indicating a value of the integer data value
5 to a base input of a modulo exponentiation block;
6 connecting a second register holding signals indicating a value of the prime modulus,
7 to a modulus input of the modulo exponentiation block;
8 connecting a third register holding signals indicating a value of the prime modulus
9 less two, to an exponent input of the modulo exponentiation block;
10 wherein the modulo exponentiation block generates an output based on a first quantity
11 modulo a value at the modulus input; and
12 wherein the first quantity substantially equals, modulo the value at the modulus input,
13 a value at the base input raised to a power of a value at the exponent input.

1 4. An apparatus for generating an output signal indicating a multiplicative inverse of an
2 integer modulo a prime modulus comprising:
3 a modulo exponentiation block configured to generate the output signal based on a
4 first quantity modulo a value at a modulus input, the first quantity
5 substantially equal, modulo the value at the modulus input, to a value at a base
6 input raised to a power of a value at an exponent input;
7 a first input for receiving a first signal indicating a value of the integer, the first input
8 connected to the base input;
9 a second input for receiving a second signal indicating a value of the prime modulus,
10 the second input connected to the modulus input; and
11 a circuit connected to the second input configured to generate on a first output a third
12 signal indicating a value of the prime modulus less two, the first output
13 connected to the exponent input.

1 5. An apparatus for performing a particular operation for using digital signatures on a
2 network, the apparatus comprising a modulo exponentiation block configured for producing a
3 multiplicative inverse of an integer modulo a prime modulus.

1 6. The apparatus as recited in Claim 5, further comprising no circuitry block configured
2 to perform an extended Euclidian algorithm (EEA) and no general-purpose processor
3 configured by instructions to perform the EEA.

1 7. The apparatus as recited in Claim 5, wherein:
2 the particular operation is performed in a series of sequential computations
3 accomplished over a corresponding series of computation cycles; and
4 the apparatus further comprises connections configured to use the modulo
5 exponentiation block during a plurality of computation cycles of the series of
6 computation cycles.

1 8. The apparatus as recited in Claim 5, wherein the particular operation is an RSA
2 encrypting operation.

1 9. The apparatus as recited in Claim 5, wherein the particular operation is an RSA
2 decrypting operation.

1 10. The apparatus as recited in Claim 5, wherein the particular operation is a digital
2 signature algorithm signing operation.

1 11. The apparatus as recited in Claim 5, wherein the particular operation is a digital
2 signature algorithm verifying operation.

1 12. A computer-readable medium carrying one or more sequences of instructions for
2 generating a multiplicative inverse of an integer modulo a prime modulus, which instructions,
3 when executed by one or more processors, cause the one or more processors to carry out the
4 steps of:
5 sending data indicating a value of the integer as an base input to a modulo
6 exponentiation function;
7 sending data indicating a value of the prime modulus as an modulus input to the
8 modulo exponentiation function; and
9 sending data indicating a value of the prime modulus less two as an exponent input of
10 the modulo exponentiation function,
11 wherein
12 the modulo exponentiation function generates an output based on a first
13 quantity modulo the modulus input, and
14 the first quantity substantially equals, modulo the modulus input, the base
15 input raised to a power of the exponent input.

1 13. The computer-readable medium recited in Claim 12, wherein the exponentiation
2 function sends the base input, the modulus input and the exponent input to a special-purpose
3 block of circuitry configured to perform modulo exponentiation.